

# Criptografía Simétrica y Asimétrica en la práctica

<b>¿Qué es la Criptografía ?</b>	<b>1</b>
Inicios pasados	1
<b>Criptografía Actual</b>	<b>1</b>
Criptografía Simétrica	1
Izarc.es	2
Criptología clave Asimétrica	4
GnuPg	5
Criptografía Función Hash	10
Hash Generator	11
Firma digital	<b>13</b>
Gpg4win (Kleopatra)	13

## ¿Qué es la Criptografía ?

- Mensajes ininteligibles para receptores no autorizados , si alguien lo intercepta, que no sepa utilizarlo.
- Garantiza la confidencialidad de la información

## Inicios pasados

Los jeroglíficos fueron los primeros, método sustitución

Escítala, los espartanos y utilizaban el método transposición

Cifrador César, utilizaban los Romanos, método de sustitución. Desplazar el alfabeto en x posiciones

## Criptografía Actual

### Criptografía Simétrica

Criptografía Simétrica o de clave Privada : Receptor y emisor conocen la clave para cifrar/descifrar el mensaje

### Ventajas

- Eficiente en grupos reducidos
- Sencillos de utilizar
- Eficientes (poco tiempo cifrar/descifrar)

### Desventajas

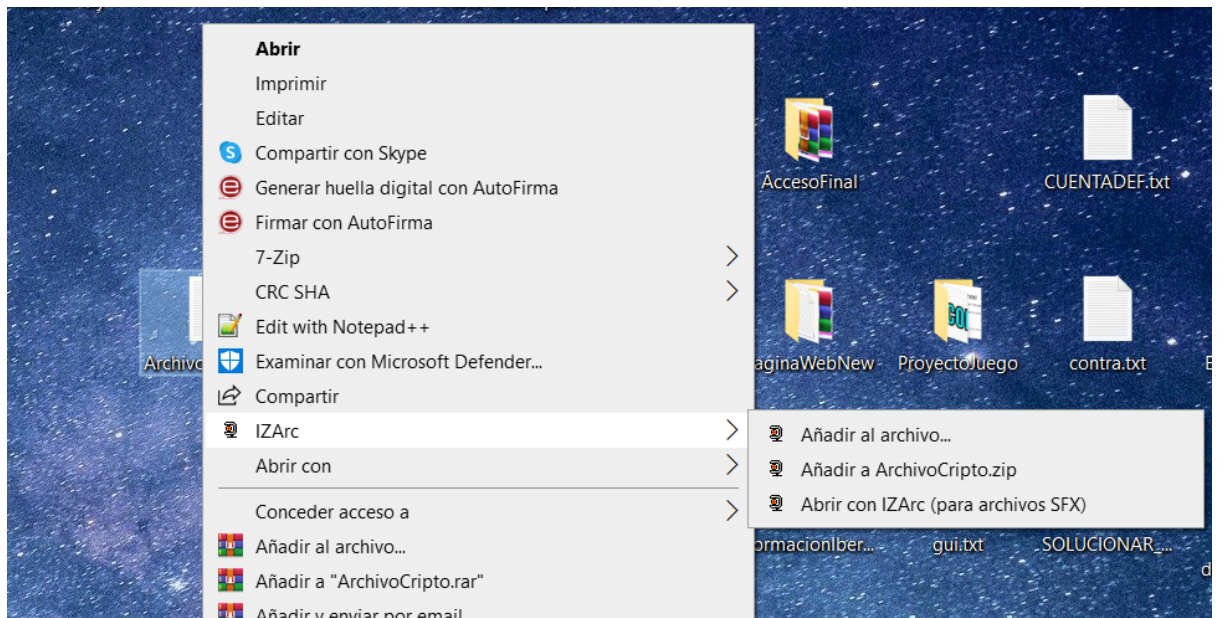
- Posible intercambio de claves por medios no seguros
- Gran cantidad de claves a memorizar/almacenar

## Izarc.es

### Herramienta Windows

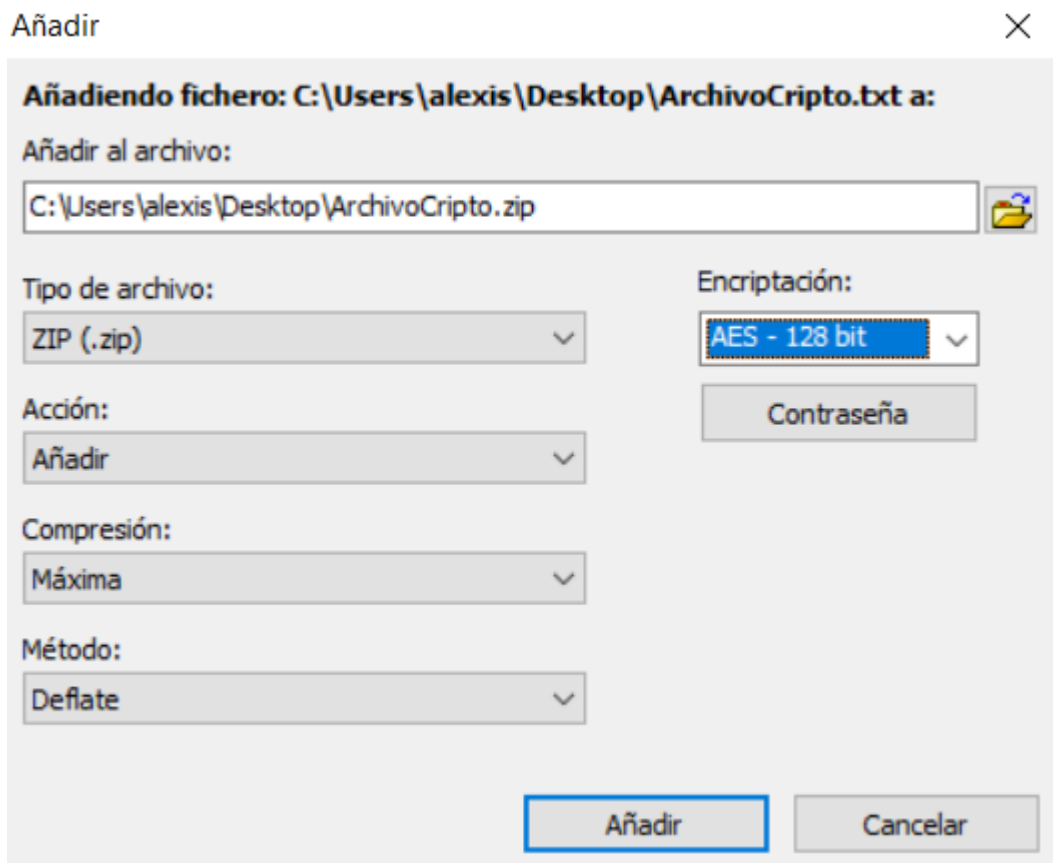
<https://izarc.es/descargar>

Una vez descargado , seleccionamos nuestro archivo a encriptar

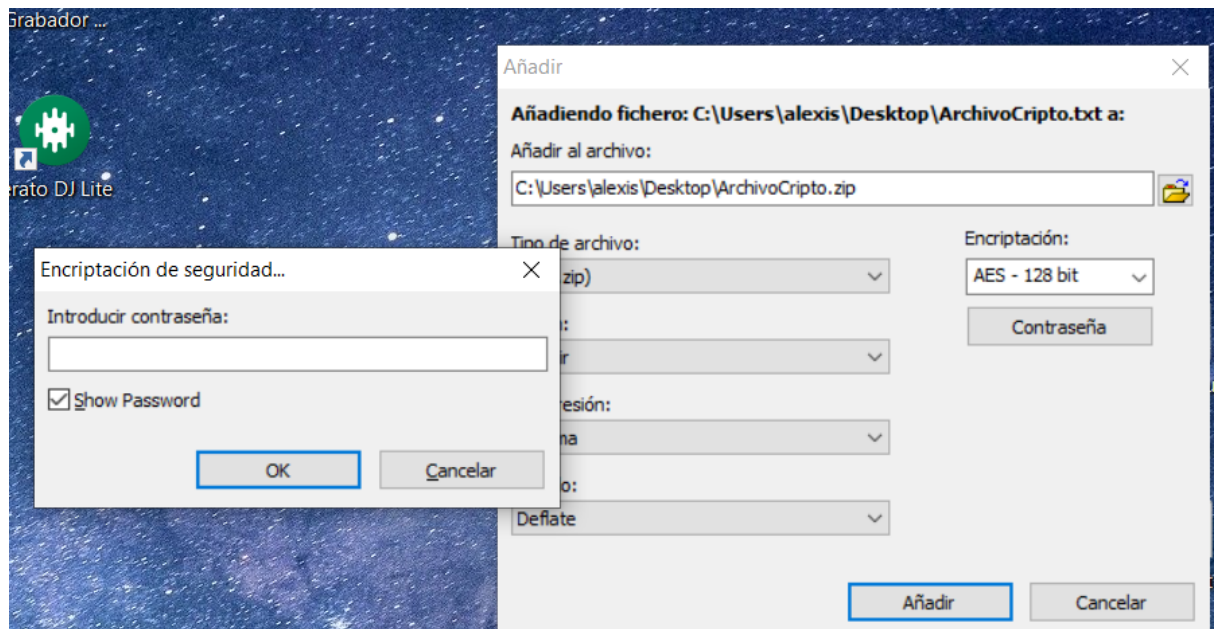


Se nos abre

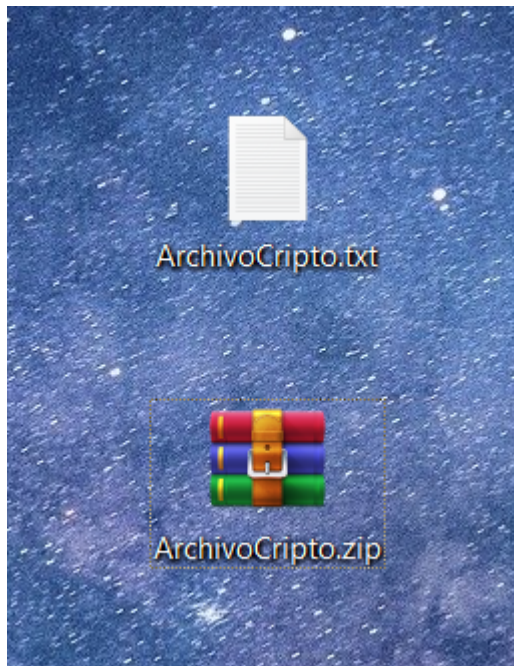
En encriptación elegimos cuantos bits queremos de seguridad



Introducimos contraseña



y ya lo tenemos encriptado el archivo.  
Se nos crea un zip con contraseña



Esto es una forma básica de encriptar con esta aplicación

## Criptología clave Asimétrica

Receptor y emisor disponen de una clave pública y otra privada para cifrar/descifrar el mensaje.

- Clave matemáticamente relacionadas
- Lo que cifras con una solo lo puedes descifrar con la otra
- Imposible deducir la clave privada con la pública



### Ventajas

- Menor número de claves
- Utilización medios no seguros
- Firma digital (no repudio)

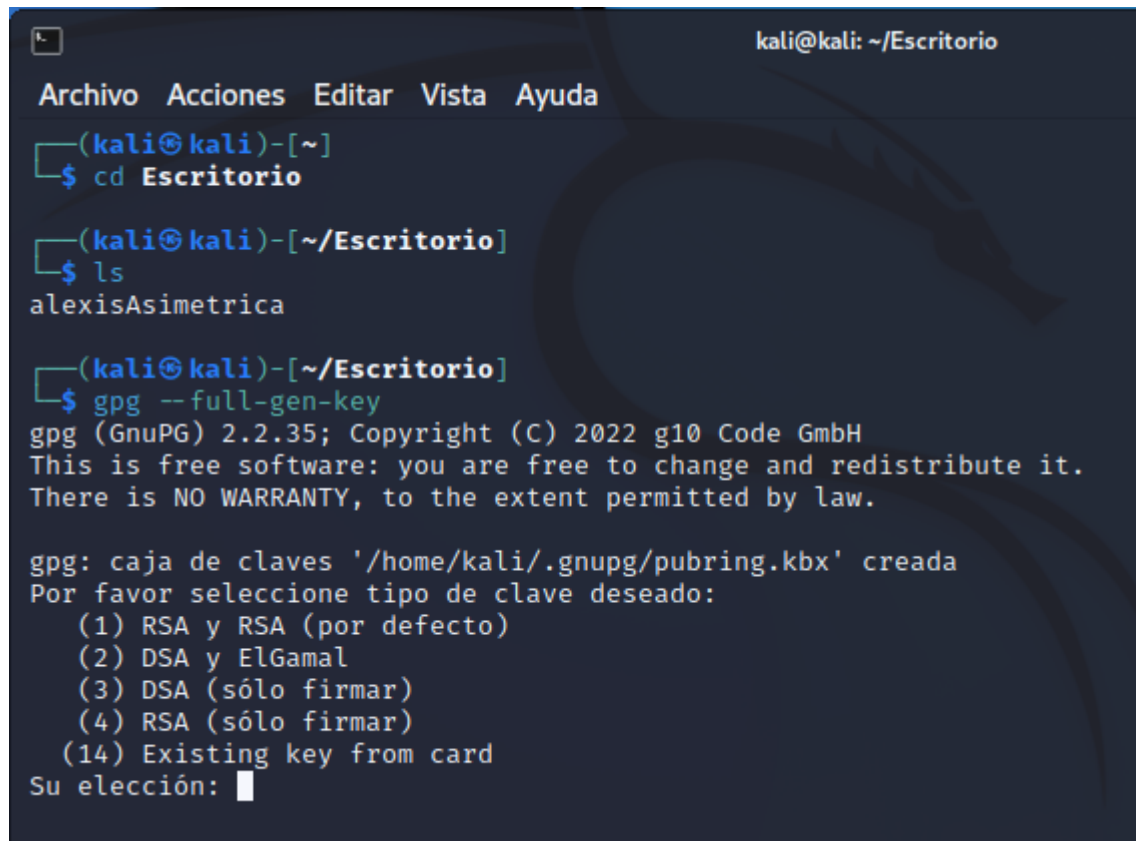
### Desventajas

- Poco eficientes
- Proteger clave privada (con criptografía simétrica)
- Importante backup de la clave privada

## GnuPg

Herramienta que nos viene incorporada en Kali Linux

Ponemos el comando **gpg --full-gen-key**



```
kali@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
(kali@kali)-[~]
$ cd Escritorio
(kali@kali)-[~/Escritorio]
$ ls
alexisAsimetrica
(kali@kali)-[~/Escritorio]
$ gpg --full-gen-key
gpg (GnuPG) 2.2.35; Copyright (C) 2022 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: caja de claves '/home/kali/.gnupg/pubring.kbx' creada
Por favor seleccione tipo de clave deseado:
  (1) RSA y RSA (por defecto)
  (2) DSA y ElGamal
  (3) DSA (sólo firmar)
  (4) RSA (sólo firmar)
  (14) Existing key from card
Su elección: █
```

```
kali@kali: ~/Escritorio

Archivo Acciones Editar Vista Ayuda

¿De qué tamaño quiere la clave? (3072) 1024
El tamaño requerido es de 1024 bits
Por favor, especifique el período de validez de la clave.
    0 = la clave nunca caduca
    <n> = la clave caduca en n días
    <n>w = la clave caduca en n semanas
    <n>m = la clave caduca en n meses
    <n>y = la clave caduca en n años
¿Validez de la clave (0)? 0
La clave nunca caduca
¿Es correcto? (s/n) y

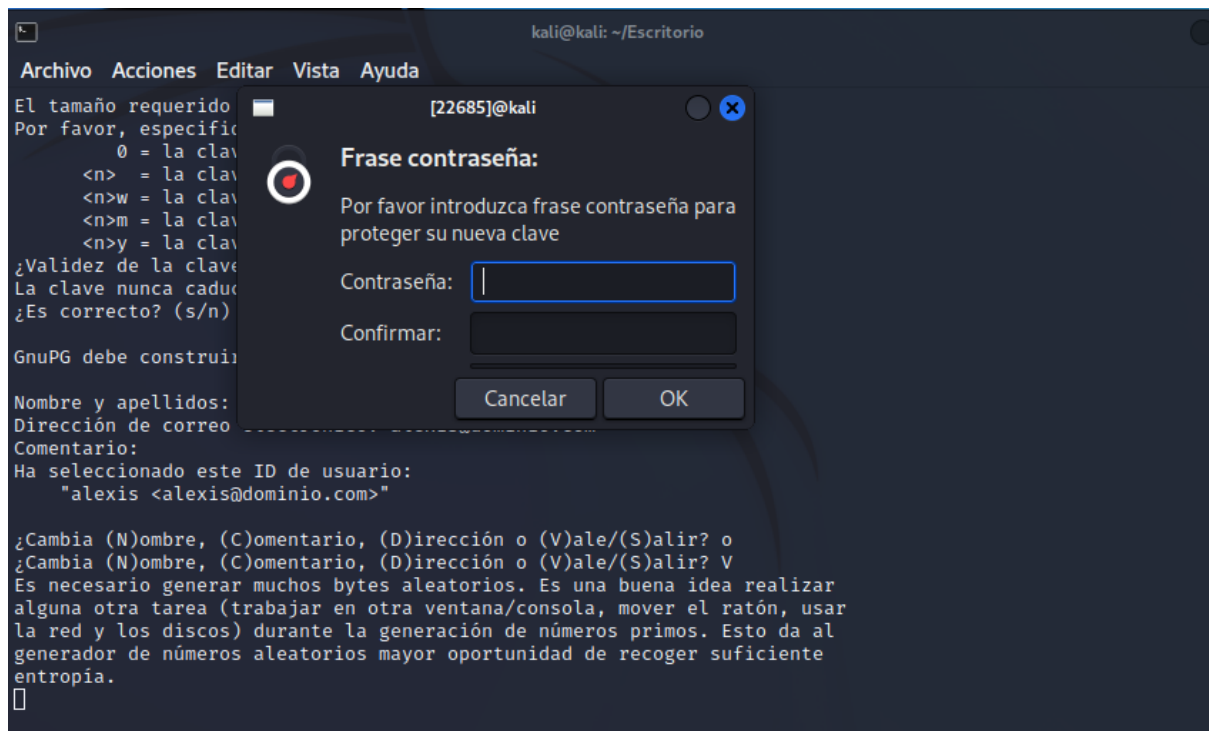
GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: alexis
Dirección de correo electrónico: alexis@dominio.com
Comentario:
Ha seleccionado este ID de usuario:
    "alexis <alexis@dominio.com>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? o
¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? V
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
```

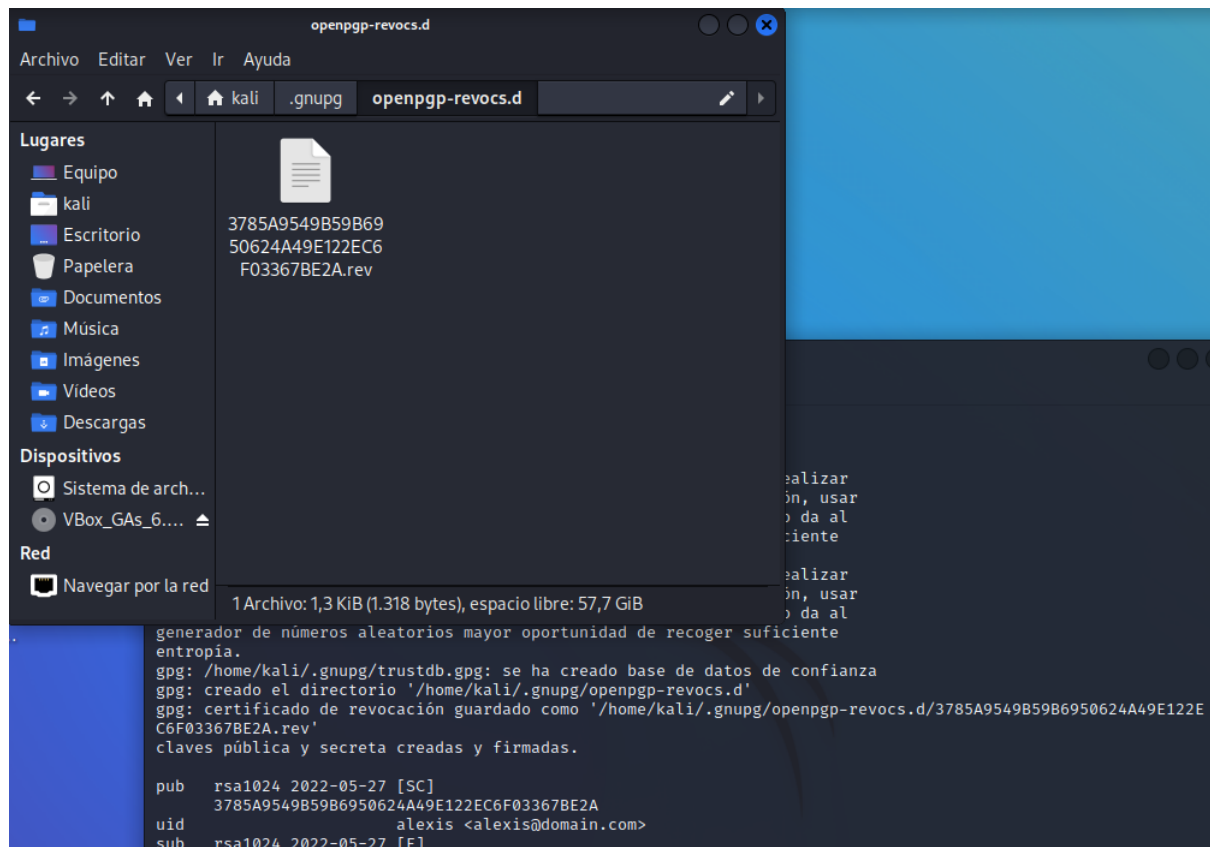
Al introducir todos los datos que nos piden , se no abre una ventana para poner una contraseña y generar el cifrado asimétrico





Se nos ha generado





Claves pública y secreta creadas y firmada



```
~/Escritorio/3785A9549B59B6950624A49E122EC6F03367BE2A.rev - Mousepad
Archivo  Editar  Buscar  Ver  Documento  Ayuda
[Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]
1 Este es un certificado de revocación para la clave OpenPGP:
2
3 pub   rsa1024 2022-05-27 [S]
4       3785A9549B59B6950624A49E122EC6F03367BE2A
5 uid   alexis <alexis@domain.com>
6
7 Un certificado de revocación es una especie de "interruptor general" para declarar
8 públicamente que una clave no debería usarse más. No es posible deshacer
9 un certificado de este tipo una vez que se publica.
10
11 Úsalo para revocar esta clave en caso de un compromiso o pérdida de
12 la clave secreta. De cualquier modo, si la clave secreta está disponible,
13 es mejor generar un nuevo certificado de revocación y dar una razón para la misma
14 Para más detalles, lee la descripción de la orden gpg "--generate-revocation"
15 en el manual GnuPG.
16
17 Para prevenir el uso accidental de este archivo se han insertado dos
18 puntos (:) antes de los 5 guiones debajo. Remueve estos dos puntos
19 con un editor de texto antes de importar y publicar este certificado
20 de revocación.
21
22 :-----BEGIN PGP PUBLIC KEY BLOCK-----
23 Comment: This is a revocation certificate
24
25 iLYEIAEKACAWIQQ3halUm1m2lQYkpJ4SLsbwM2e+KgUCYpEwCgIdAAAKCRASLsbw
26 M2e+KrfiA/9KijU+d3NCNKo3/eV2t+gOaQjQM2mgHntp109+CsdadjmTimdPj1Wm
27 rExR0otnC0CcUIYVz0A1+sGTxra/PVZ8hZ+urFH3RBf7/zurRMyA1eD68T6ujUhf
28 2jV3KILXJTqw931HnYim2XsWTrmIyWhD08HIGuHCftCk7I3o7Pw2oA==
29 =vUPr
30 -----END PGP PUBLIC KEY BLOCK-----
31
```

Para saber que keys tengo creadas

```
(kali㉿kali)-[~/Escritorio]
$ gpg --list-keys
gpg: comprobando base de datos de confianza
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: nivel: 0  validez: 2  firmada: 0  confianza: 0-, 0q, 0n, 0m, 0f, 2u
/home/kali/.gnupg/pubring.kbx

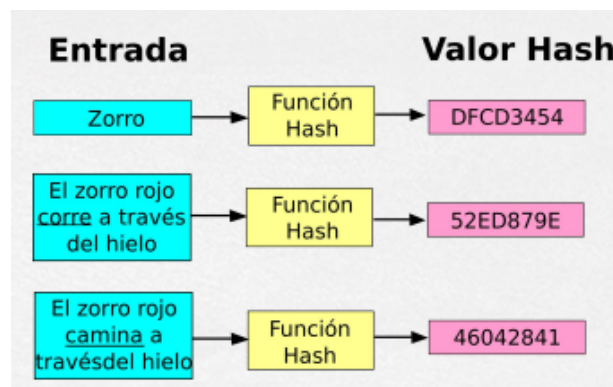
pub   rsa1024 2022-05-27 [SC]
      3785A9549B59B6950624A49E122EC6F03367BE2A
uid   [ absoluta ] alexis <alexis@domain.com>
sub   rsa1024 2022-05-27 [E]

pub   rsa1024 2022-05-27 [SC]
      E9FEB100013D7CA03BF222F5E4DFDDCA0746B6F4
uid   [ absoluta ] Alexis2 <alexis2@domain.com>
sub   rsa1024 2022-05-27 [E]
```

## Criptografía Función Hash

- Algoritmo (operaciones matemáticas, lógicas,...)
- Transforma unos datos en una serie de caracteres con longitud fija
  - Genera un valor a partir de una cadena de texto utilizando una función matemática
  - Identifica de forma única a un fichero, disco duro,...

Es decir, asignar un dni único a unos datos.



- Protege la integridad de los datos



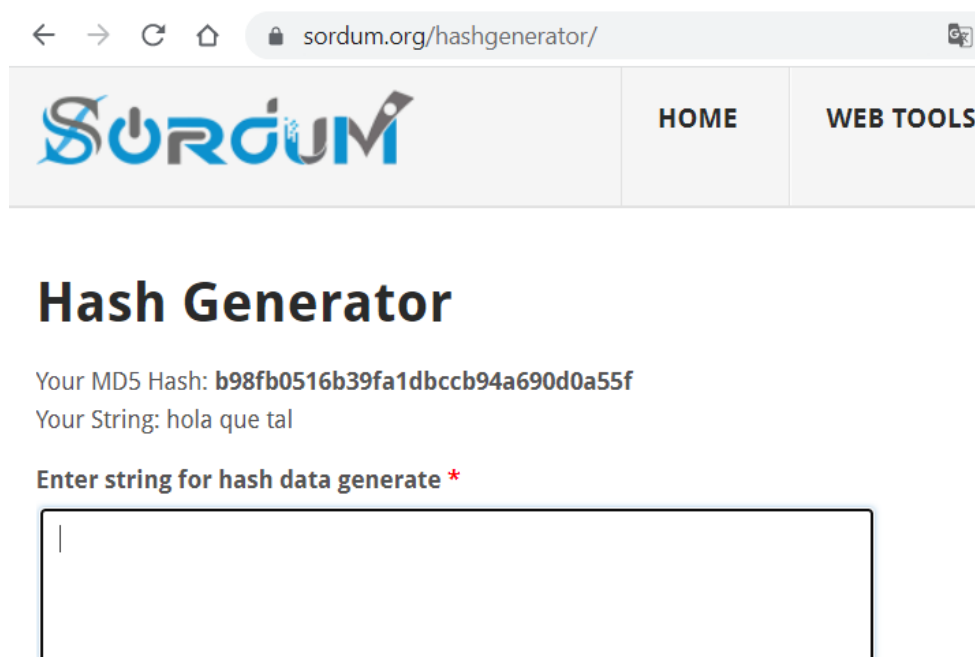
- Principales Algoritmos
  - MD5, SHA
- Reglas
  - Números generados con un mismo método tienen igual tamaño
  - Imposible reconstruir texto base a partir del Hash

- Computacionalmente sencillo de calcular
- Ejemplo: Un sospechoso a la hora de interceptar su ordenador, se le hace un código hash para que a la hora de llevarlo al juez se compare.  
Si el código hash coincide es que no se a modificado el disco duro , si cambia es que los datos fueron manipulados.

## Hash Generator

Los hay online y para instalar

Para añadir hash a un texto:

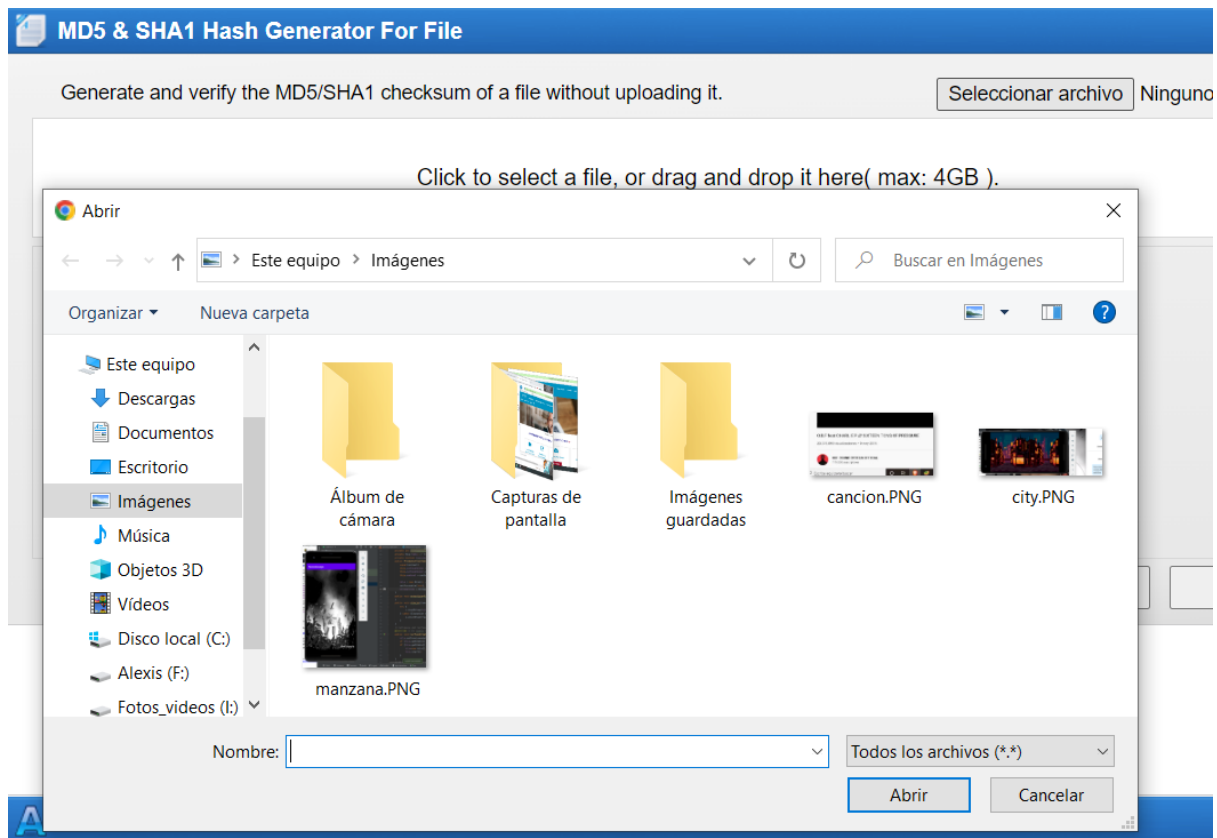


The screenshot shows a web browser window with the address bar displaying 'sordum.org/hashgenerator/'. The website has a header with the 'SORDUM' logo and navigation links for 'HOME' and 'WEB TOOLS'. The main content area is titled 'Hash Generator' and displays the following information:

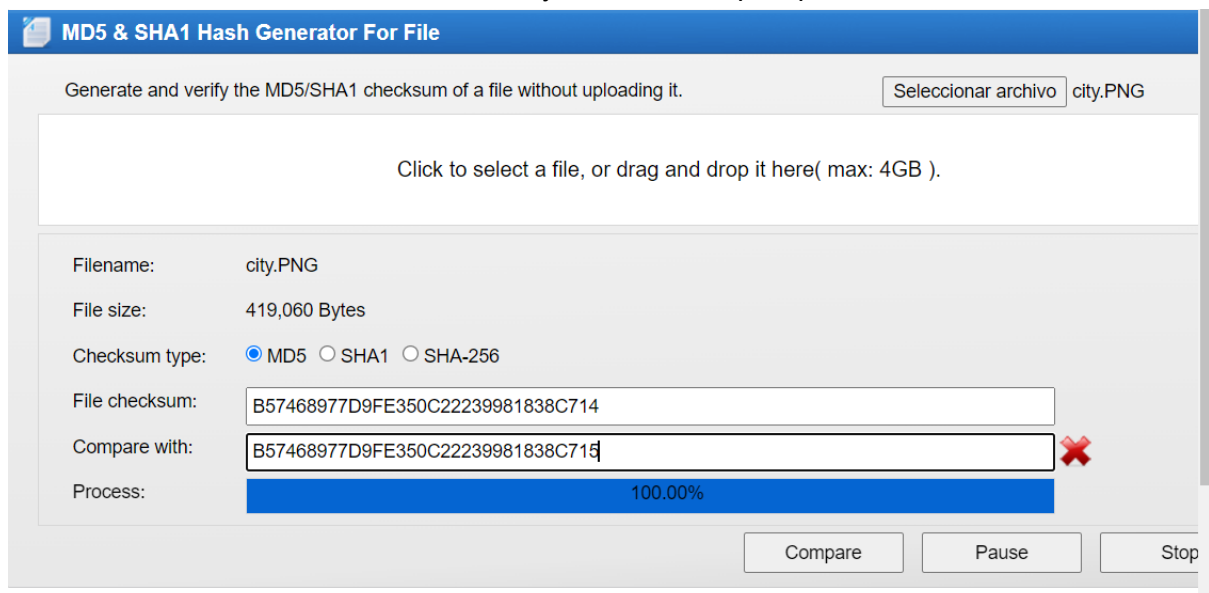
- Your MD5 Hash: **b98fb0516b39fa1dbccb94a690d0a55f**
- Your String: hola que tal
- A label 'Enter string for hash data generate \*' above a large, empty text input field.

Generar Hash de un archivo

Seleccionamos el archivo que queremos

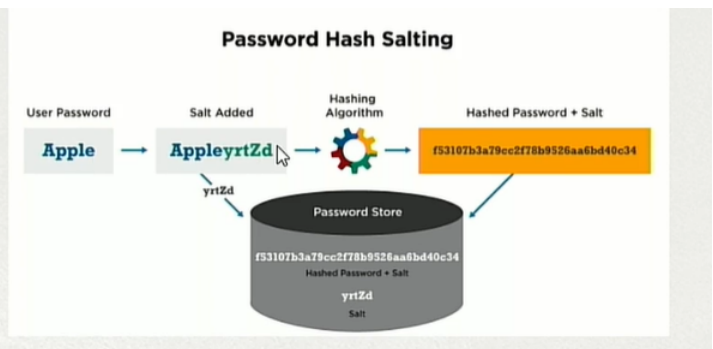


Se ha generado el código hash y se puede comparar con otro archivo y su hash.  
En este caso al cambiar solo un carácter ya no coincide por que el hash es un dni único.



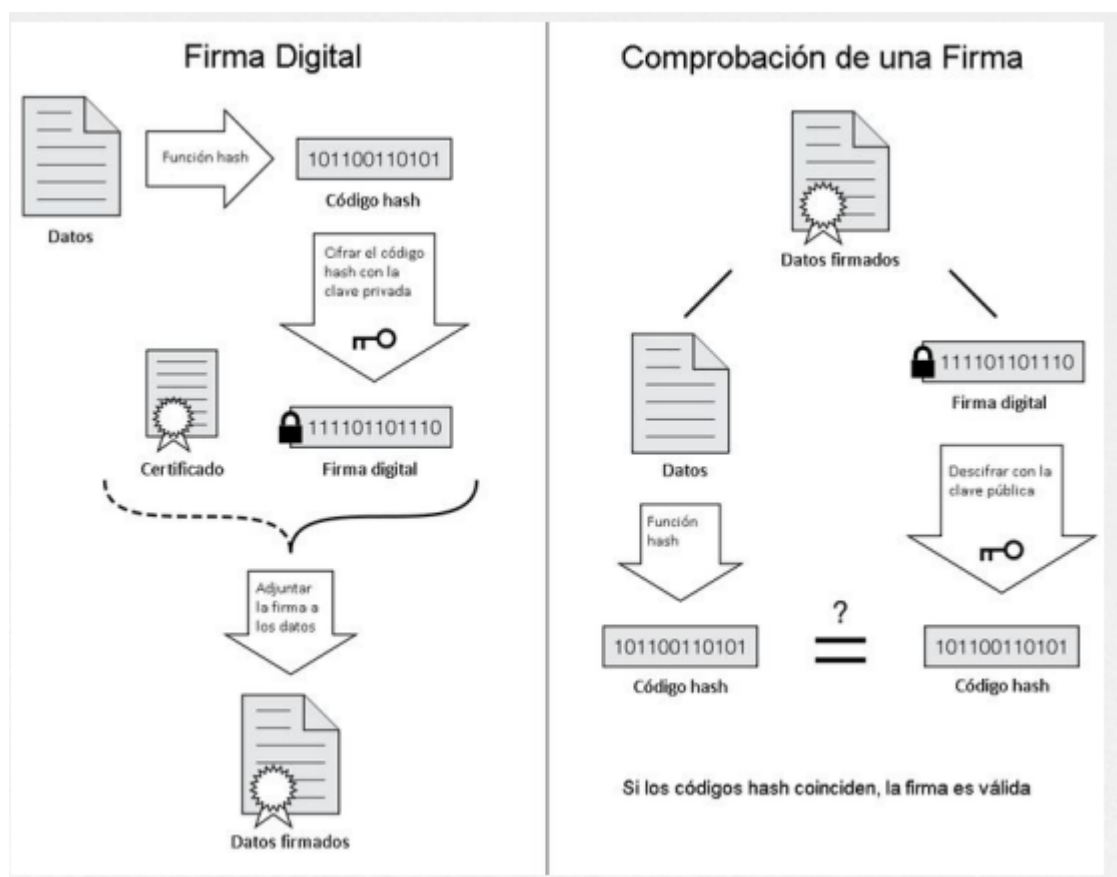
- Reverse hashing

ID	user_login	user_pass
1		\$P\$BvVWVtZxwlg8xLjQmCnNPGSR1
2		\$P\$BaRLbcbfbqZ7z9VwZWYig8svTG31
3		\$P\$B4qOthegJY3JZv6 bK4A40Br3SuxCF1
4		\$P\$B0IDCzLk494sOXZaZK9KEKzsvh4l
5		\$P\$B6cWxeer1AFH8ogYov7FIAayY4trM00



## Firma digital

La firma digital lo que hace es coger los datos y los aplica una función hash



Gpg4win (Kleopatra)

<https://gpg4win.org/thanks-for-download.html>

Añade diversas herramientas , el que usaremos es el de Kleopatra



Abrimos Kleopatra, le damos a “Nuevo par de claves” e introducimos nuestros datos, le damos a crear.

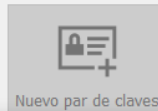
**Bienvenido a Kleopatra Gpg4win-4.0.2**

Kleopatra es una interfaz para el software de cifrado [GnuPG](#).

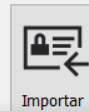
Para la mayoría de las acciones necesita una clave pública (certificado) o su propia clave privada.

- La clave privada no es necesaria para descifrar o firmar.
- Otras personas pueden usar la clave pública para verificar su identidad o cifrar para usted.

Puede aprender más sobre esto en la [Wikipedia](#).



Nuevo par de claves



Importar

**Asistente de creación del par de claves****Introduzca detalles**

Por favor, introduzca sus detalles personales debajo. Si desea más control sobre los parámetros, pulse el botón «Configuración avanzada».

Nombre:  (opcional)

Correo:  (opcional)

☐ Proteger la clave generada con una frase de contraseña.

alexis <alexis@alexis.com>

[Configuración avanzada...](#)

[Crear](#)

[Cancelar](#)



← Asistente de creación del par de claves

## Par de claves creado correctamente

Su nuevo par de claves se ha creado correctamente. Consulte los detalles sobre el resultado y algunos pasos a seguir sugeridos más abajo.

### Resultado

Par de claves creado correctamente.  
Huella digital: E92A 0471 656E D189 E781 7165 20F3 4150 7086 1CD6

### Siguientes pasos

Hacer copia de respaldo de su par de claves...

Enviar clave pública por correo...

Enviar clave pública a un servicio de directorio...

Finish

Nos da la opción de firmar o cifrar  
En nuestro caso le damos a firmar

Kleopatra

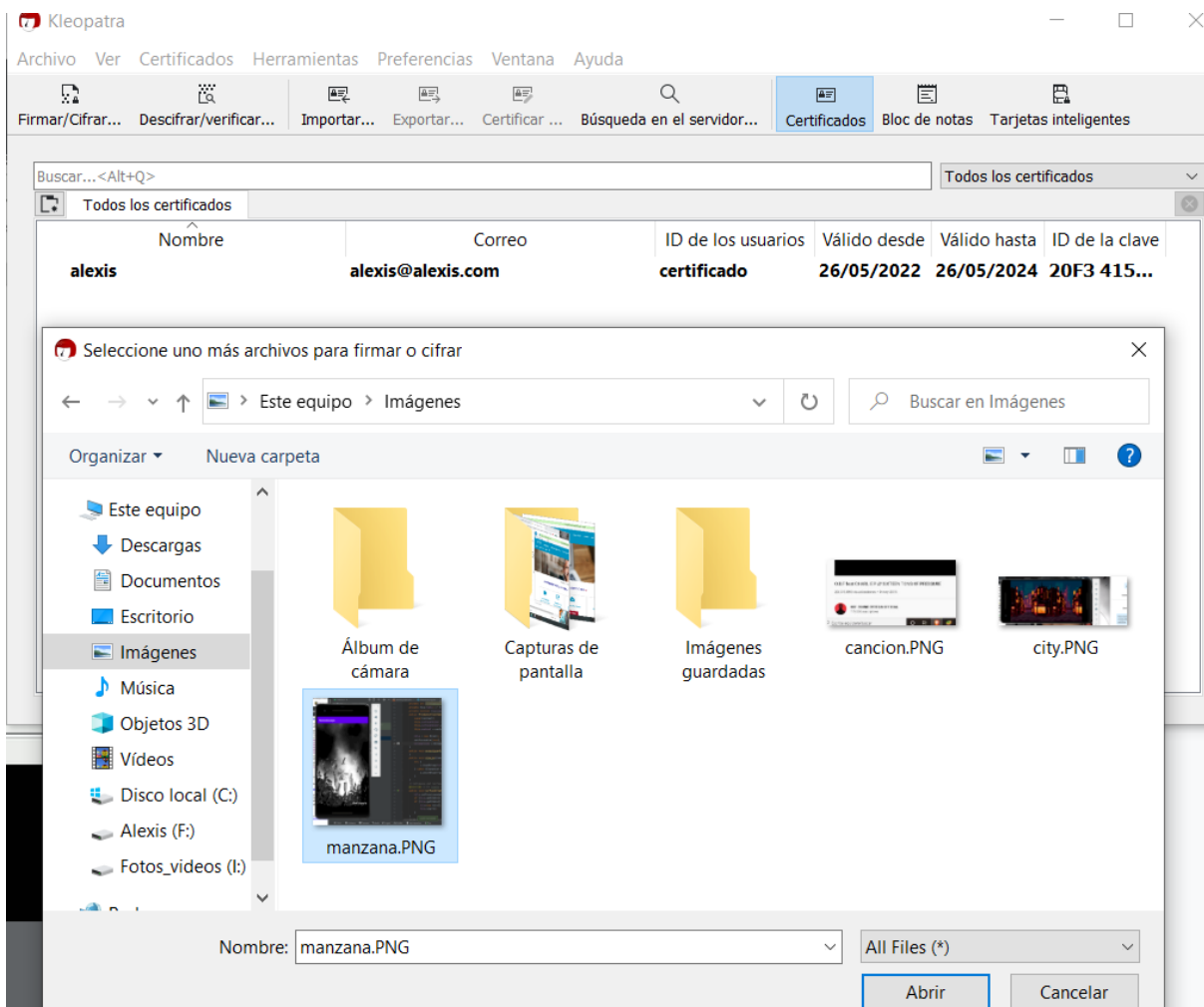
Archivo Ver Certificados Herramientas Preferencias Ventana Ayuda

Firmar/Cifrar... Descifrar/verificar... Importar... Exportar... Certificar ... Búsqueda en el servidor... Certificados Bloc de notas Tarjetas inteligentes

Buscar... <Alt+Q> Todos los certificados

Nombre	Correo	ID de los usuarios	Válido desde	Válido hasta	ID de la clave
alexis	alexis@alexis.com	certificado	26/05/2022	26/05/2024	20F3 415...

Elegimos el fichero que queremos firmar



## Firmar o cifrar archivos

Probar autenticidad (firmar)

☒ Firmar como: ✓ alexis <alexis@alexis.com> (certificado, created: 26/05/2022) ▾

Cifrar

☐ Cifrar para mí: ✓ alexis <alexis@alexis.com> (certificado, created: 26/05/2022) ▾

☐ Cifrar para otros: ✗ Por favor, introduzca un nombre o dirección de correo... 

☐ Cifrar con contraseña. Cualquier persona con la que comparta la contraseña podrá ver los datos.

Salida

Archivos/carpeta de salida:

 C:/Users/alexis/Pictures/manzana.PNG.sig  

☐ Cifrar o firmar cada archivo por separado.

Firmar

Cancel

### Resultado

El estado y progreso de la operación de cifrado se muestra aquí.

OpenPGP: Todas las operaciones terminadas.

manzana.PNG → manzana.PNG.sig: **Firmado correctamente.**

Finish

Cancel

Se nos ha creado la firma digital de ese archivo

